Abstract

A method and apparatus for configuring a network security system. A registry data structure includes useful information about the network, such as definitions of roles within the network. The registry may also include information regarding the topology of the network. Documents that contain network security policies are linked to the registry data structure. The policy documents may then be transformed into device-specific configuration documents using a document transformation algorithm, which takes a document of a certain format as input and generates a document in a different format as output. Various different scripts may control the transformation process to achieve compatibility with security devices from different vendors. An advantage of the invention is that major network management tasks, including policy enforcement, may be done by document transformations. Once adopted, a security strategy may be changed in order to adapt to changing business requirements.